Brief Analysis of Constitutionality of Section 12 (F) of Data Protection Bill

Deeksha Sabharwal[1]

Abstract

India will be becoming a digital economy of 1 trillion, implies that its value will be equivalent to 18-23 percent of nation's nominal GDP.[2] Since digital reliability is increasing rapidly, it becomes crucial to have laws and regulation regarding digital space. Working for the same, a personal data protection bill was introduced in Parliament on December 11th, 2019. The bill will be necessary for governance due its 'protective' nature. This paper will analyse Section 12(f) of the bill in the light of constitutional principles. The Supreme Court of India, in the case of R. Rajagopal v. State of Tamil Nadu[3] has held that citizens have the right to protect their privacy and the publication of personal information without consent regardless of the nature of content of such publication may violate the privacy of the person concerned. But the case also noted that publication of information which is available in the public domain does not violate the right to privacy of concerned individuals. The paper attempts to suggest the loopholes and relevant suggestions which are in consonance with rule of law.

I. Introduction to key Terminologies of the Data Protection Bill

The Personal Data Protection bill was drafted after the recommendations of Justice B.N. Srikrisna Committee report. The committee analysed the need of law for protection of rights of individuals in an era of rapidly expanding digital economy. The draft prepared by committee strictly kept regard to privacy of individuals and guidelines of *Aadhar Case.*[4] However, the author analysed some inconsistencies in the bill. In the current research stress is placed upon determining the constitutionality of Sec. 12(f) of the bill. Noteworthy, the dubitable provision was nowhere mentioned in the bill, even after the introduction of the bill, Srikrisna J. advocated the review of bill due to his disappointment by the provisions and went on to state that the provisions of bill may lead to Orwellian state.[5]
Since the bill is technical it is crucial to introduce the key terminologies which are used throughout the bill, these terminologies will also provide a fair idea of the theme of the bill.

a. **Personal Data[6]-** Any data which can lead to identification of an individual may be termed as personal data, as noted by the draft committee that with regard to the pace of technological advancements, it would be in the interest of justice to have a broad definition of the term 'Personal Data'. Further, the bill fails to differentiate between some technical terms, like - De-identification, Pseudonymisation, Anonymisation. The latter two terms fall on a high spectrum where the de-identification ends. Pseudonymisation refers to granting a fictional identity to data principle in order to retain his privacy, while Anonymisation refers to nullifying the identity of the data principle. De-identification, which is mentioned in Sec.

[1] Deeksha Sabharwal - Fourth Year, B.A. LL.B. Manipal University, Jaipur.
[2] Rajat Gupta, Boom in the Digital Economy (04/04/2020) https://www.thehindubusinessline.com/info-tech/digital-economy-a-1-trillion-opportunity-for-india/article26323 150.ece
[3] R. Rajagopal v. State of Tamil Nadu, 6, SCC 632
[4] (2017) 10 SCC 1.
[5] Mayank Tripathi, Personal Data Protection (05/04/2020) https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms?from=mdr
[6] Personal Data Protection Bill, § 2(28) 2019.

2(16) of the bill, refers to scattering the data collected in such a manner that it becomes difficult to reconcile it. However, if the high-end barrier is set which requires the re-identification to be an impossible process then it will be practically difficult and it may affect potential benefits which are obtained from data sets.

b. **Sensitive Personal Data[7]-** Although measures are present for protection of personal data, then also to minimise the possibility of the misuse of the data which can cause relatively greater harm to the data principle this category is created. Due to absence of any straight-jacket formula for determination of sensitive personal data, due regard is given to the contextual approach, according to which the nature of the data i.e., whether it is personal data or sensitive personal data depends on the circumstances from case to case but then this will put an extra burden on data fiduciary to determine if a case contains sensitive personal data or not. Therefore, a better approach has been adopted by the drafters, it listed a non-exhaustive type of personal information which will also give liberty to data fiduciary to determine the case apart from the list.

c. **Consent[8]-** Consent basically means, with regard to instant bill, a right granted to data fiduciary by the data principle to access the information which is relevant for the specific purpose, Sec. 2(10) and Sec. 2(11) deals with formalities of consent. If we consider regular forms of digital consent, it is mainly obtained by the software one signs in, the applications one downloads and websites one access. As mentioned by the draft committee these forms of consent are often boilerplate. Generally, they are such that it is not convenient to read them by a layman, if it is readable then it is tough to understand, and even if one understands these terms are non-meaningful in isolation.

d. **Data Principal[9]-** The person whose data is being processed for the purpose of common public good and in propagation with free and fair digital economy, is to be known as Data Principle and the term 'principal' emphasizes on the importance of autonomy of Individual's Data.

e. **Data Fiduciary[10]-** Data Fiduciary refers to a person, State, company or any Juristic entity to process the data. The abovementioned authorities are expected to act reasonably and take the step which is in the best of interest of the Data Principal.

f. **Difference between Privacy and Anonymity -** Although both the terms 'Privacy' and 'Anonymity' sound a lot similar but a difference is made between the two.[11] Both anonymity and privacy do not let the third-party gain access to data but both follow a different approach for the same purpose. Privacy refers to concealment of information, whereas Anonymity refers to concealment of the identity of the data principle. An authorised access to data of individuals will amount to breach of privacy while the case where the government collects the data in advancement of national interest or public good

[7] Personal Data Protection Bill, § 2 (36) 2019.
[8] Personal Data Protection Bill, § 2 (10) 2019.
[9] Personal Data Protection Bill, § 2 (14) 2019.
[10] Personal Data Protection Bill, § 2 (13) 2019.
[11] Jeffrey M. Skopek, Reasonable Expectations of Anonymity ,101 Va.l.rev. ,691-762 (2015).

will serve as legitimate state interest. If the State preserves the anonymity of the individual it could legitimately assert a valid State interest in the preservation of public health to design appropriate policy interventions on the basis of the data available to it. Apart from this, it becomes immensely important to put checks on the procedure and reasoning of the government in collection of data, in order to sing with the spirit of the Constitution.

II. Relation Between Right to Privacy and Digital Informational Privacy

Earlier there was confusion as to whether Right to Privacy is a guaranteed fundamental right or not, before *Aadhar case*[12], *M.P. Sharma and Others v. Satish Chandra Distt. Magistrate, Delhi and Others*[13] (the eight-judge bench stated that right to privacy is not a Fundamental Right) and *Kharak Singh v. State of U.P.*[14] discussed the scope of right to privacy as a fundamental right. Recently, in 2017 the *Aadhar Case*[15] clarified that right to privacy is a fundamental right protected under Arts. 14, 19 and 21. Right to privacy covers a wide range of non-exhaustive list of the sub-topics covered under it, for example, concept of privacy may be subjective with respect to time-frame, back in 19th century it may be irrelevant to discuss the concept of data privacy and breach of privacy by paparazzi might seem to be a greater concern but when the world is being dependent of digitised data then it becomes crucial to introduce the data protection legislation with utmost care, deviating from which may lead to destruction of welfare state.[16]

It is important to note that privacy has both positive and negative content. The negative content restrains the State from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the State to take all necessary measures to protect the privacy of the individual.[17] Introducing an error-ridden bill will be unjust behaviour with both the content.

Another facet of Right to Privacy is the Informational privacy, which is based on the fact that every transaction or digital step by an individual leaves some marks which can be traced without her knowledge, if seen in isolation then these silos do not constitute substantial information but when combined then it can be a serious threat to privacy of an individual. This right needs to be protected from both state and non-state instrumentalities. Every individual should have a right to be able to control exercise over his/her own life and image as portrayed in the world and to control commercial use of his/her identity.[18] And this is the affair which shall remain private in order to make it convenient for the concerned individual to live his regular life most possible convenience. Right to privacy encompasses the right to informational and data privacy in it.[19] In a digital society an individual has the right to protect herself by controlling the dissemination of such personal information.[20] All the fundamental rights enshrined under Part III of the

[12] (2017) 10 SCC 1.
[13] 1954 SCR 1077.
[14] AIR 1963 SC 1295.
[15] (2017) 10 SCC 1.
[16] Supra note 4.
[17] Justice (Retd.) K.S. Puttuswamy v. Union of India, 10, SCC 1, 153,
[18] Justice (Retd.) K.S. Puttuswamy v. Union of India, 10, SCC 1, 152
[19](2017) 10 SCC 1.
[20] Justice (Retd.) K.S. Puttuswamy v. Union of India, 10, SCC 1, 305

constitution are safeguards against the state, these are considered the utmost important parameters of a civilized society. Similarly, privacy concerns arise when the State seeks to intrude into the body and the mind of the citizen and recently the state has continuously tried to encroach individual privacy by the way of legislations like Aadhar Act and Personal Data Protection Bill. It is noteworthy that there is provision for the liability for negligence by private entities but no such provisions are available for the government. S. 43A of the Information Technology Act of 2000 contains the provisions where there is liability for the private bodies regarding damages and compensation.

IV. Brief Analysis of Constitutionality of Section 12(f) of the Bill

a. Violation of Right to Life

The preamble of the bill recognizes the right to privacy as a Fundamental Right[21], which was laid down in Justice *K.S. Puttuswamy (Retd.) v. Union of India.*[22] The reading of preamble further strengthens the protective nature of the bill. The right of the person, whom data is being processed, must be protected according to the preamble. One aspect of privacy is considered the right to control the dissemination of personal/sensitive personal information.

And that every individual should have a right to be able to control exercise over his/her own life and image as portrayed in the world and to control commercial use of his/her identity.[23] The right to disseminate hence becomes a natural right not bestowed by the State. This is an inherent right of human beings, regardless of their class, strata and other factors. This aspect of informational privacy was also touched in Aadhar case[24], where Nariman J., stated that;

> 'Informational Privacy does not deal with a person's physical being directly but it affects mental health of an individual and that is why unauthorized dissemination of personal information may lead to breach of right to privacy which establishes that the bill is violative of Art. 21.'

Noteworthy, the European Court for Human Rights already stated that mere storing of personal information may amount to violation of Article 8, and since Article 8 of ECHR is in *pari materia* with the constitution the same must be applied to impugned legislation. In case of Federal Census Act Case (Volksz hlungsurteil)[25] where the court held that the combination of personalized statistical data could lead to identification of an individual which will affect the right to informational self-determination of concerned persons and hence the legislation was struck down.

Apprehension of a democracy being converted into the totalitarian state may arise if S. 12(f) is allowed to operate. The reason being that S. 12(f) is anathema to the democratic principles and rule of law, which is the bedrock of the Indian Constitution. Sec. 12(f) is *prima facie* based on

[21] Preamble of Personal Data Protection Bill, 2019.
[22] (2017) 10 SCC 1
[23] Justice (Retd.) K.S. Puttuswamy v. Union of India, 10, SCC 1, 73
[24] (2017) 10 SCC 1.
[25] (1983) 65 BVerfGE 1.

compelling state interest rather than legitimate state interest. Noteworthy, while dealing with the issue of state interest, Chandrachud, J. has formulated the test of legitimate state interest, while, Chelameswar and Sapre, JJ., were inclined in favour of the test of compelling state interest, which serves larger public interest in lieu of legitimate state interest, as a permissible restriction on a claim to digital privacy of an individual a more lenient test. However, due to the inclination of the majority towards legitimate state interest, the minority has also virtually adopted the same test. Since the test of legitimate state interest is applicable rather than the test of compelling state interest, it becomes necessary for the state to justify all the processing of the personal data.

b. The Bill Does Not Fulfil The Test Of Proportionality

It was held in Aadhar case that "Right to privacy cannot be impinged without a just, fair and reasonable law. It has to fulfil the test of proportionality i.e. (i) existence of a law (ii) must serve a legitimate State aim and (iii) proportionate."[26]

Section 12 (f) of the proposed bill[27] states tha**t*;***

> *"Notwithstanding* anything contained in section 11, the personal data may be processed if such processing is necessary, —
> (f) to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order."

Now it is doubtful whether the data of any individual exhausts to the data processor or others too. The *prima facie* reading of the impugned provision clearly set forth the message that the data for "any individual" may be processed without consent. Instant provision is clearly compromising the right of one individual over the right of another individual without any concrete basis. "Providing assistance or services" cannot be granted as a legitimate escape for stripping right of one over another. Further, the presence of the term "any individual" includes non-citizens and anti-societal elements, and compromising data of any person for service to the person who is not equivalent will amount to inequality.

> "The expression "arbitrary interference" can also extend to interference provided for under the law. The Introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims, and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances."[28]

The objectives laid down in the bill ensure the protection of privacy of an individual in furtherance of a free and fair digital economy and remedies for unauthorised processing of data, ironical to the impugned provision the preamble also commit to set a relation of trust between data principle and data fiduciary. It can be safely stated that the bill is in contravention with the very objectives that it set forth.

---

[26] (2017) 10 SCC 1.
[27] Section 12(f), Personal Data Protection Bill, (2019) https://www.prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf
[28] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, Article 8, (1981).

There is an immense importance of the requirements of clarity, accessibility, and precision when the case is of communication surveillance. The reason for this is the destructive nature of communication surveillance towards the essence of democracy as the European Court of Human Rights recognised as early as 1978.[29]

The Court found that the "mere existence" of legislation that allowed a system to secretly monitor communications gave rise to a "menace of surveillance" which amounted to a compromise with the privacy of all those to whom legislations may have been applied. Same is the case with impugned provision, it opens the risk of compromising with the data of individuals without any adequate responsibility of the state agency. ECtHR issues some threshold guidelines which deal with minimum safeguards of surveillance law to be compatible with Article 8 of ECHR.

V. Conclusion

It is of utmost importance to have legislation for the governance of private data protection, step in furtherance of this by the State deserves appreciation but the lacunas present in legislation makes it a bad law in the eye of constitution. There are some thresholds which every legislation must pass. Though main principles, as set generally, are duly fulfilled but the impugned provision suffers disability to deserve a constitutional nod. A standard degree of privacy is important for the well-being and growth of an individual. The restrictions imposed on the state to pry into the lives of the citizen goes down to affect the essence of a democratic state. This Article attempts to challenge the constitutionality of Sec.12(f) in brief. The bill shall be reviewed by a panel of experts, each from the technical and legal sector. Some provisions other than Sec. 12(f) need the attention of policymakers such as Sec. 35 of the bill allowing the exemption of several agencies of the state as specified by the central government but exempting any government agency from this bill will defeat its purpose.[30] Any deviation from the principles of rule of law and basic structure may lead to harmful consequence, these consequence may not seem great concern to some class of people but consecutive violation of established democratic principle may lead to great damage soon, hence it is essential to hold these establish principle as guiding light to ensure welfare and development of a democratic society.

[29] Klass and others v. Germany, no. 5029/71 (ECtHR: 1978).

[30] https://www.business-standard.com/article/economy-policy/govt-messed-up-control-mechanisms-b-n-srikrishna-on-data-protection-bill-120013001855_1.html last accessed on 04/04/2020.